

TW 420796

中華民國專利公報 [19] [12]

[11]公告編號：420796

[44]中華民國 90 年 (2001) 02 月 01 日
發明

全 2 頁

[51] Int.Cl⁰⁶: G09C1/00
G06F3/00

[54]名稱：設有可攜帶式電子鑰匙之電腦系統

[21]申請案號：088100448

[22]申請日期：中華民國 88 年 (1999) 01 月 13 日

[72]發明人：

王漢哲

台北市恭順街十六巷二十之一號二樓

張明智

台北市北投區火業路五一六巷十號

[71]申請人：

致伸實業股份有限公司

台北縣汐止鎮康寧街一五九號六樓

[74]代理人：許鍾迪 先生

1

2

[57]申請專利範圍：

1. 一種電腦系統，包含有：

一記憶體，用來儲存程式或檔案；
一處理器，用來執行或處理該記憶體
中之程式或檔案；一加／解密程式，用來對一程式或檔
案進行加密或解密；

一鑰匙埠；以及

一電子鑰匙(electronic key)，以可插拔
的方式連接於該鑰匙埠，其包含有一
可程式記憶體，用來儲存密碼；其中當一使用者欲對一程式或檔案進
行加密時，該加／解密程式會依據一
密碼對該程式或檔案進行加密並將該
密碼存入該鑰匙之記憶體中，而當該
使用者欲對一程式或檔案進行解密
時，該加／解密程式會自該鑰匙之記
憶體中找尋一相對應之密碼，若該密
碼存在且為一正確之密碼，則該加／
解密程式會對該程式或檔案進行解
密。2. 如申請專利範圍第 1 項之電腦系統，其
另包含有一輸入裝置，用來供該使用
者對該加／解密程式輸入或更改一密
碼。5. 3. 如申請專利範圍第 2 項之電腦系統，其
中該輸入裝置係為一鍵盤。4. 如申請專利範圍第 1 項之電腦系統，其
中該可程式記憶體係為一 EEPROM，
因此使該鑰匙不需使用電池來維持該
可程式記憶體內之資料。5. 5. 如申請專利範圍第 1 項之電腦系統，其
中該鑰匙埠可為一串聯埠(serial port)或
USB(universal series bus)埠。6. 6. 如申請專利範圍第 1 項之電腦系統，其
中該鑰匙係為一可產生游標控制訊號
之滑鼠(mouse)。7. 7. 如申請專利範圍第 1 項之電腦系統，其
中該鑰匙則係為一記憶體卡(memory
card)，其外前端設有一端連接頭用來
將其內之可程式記憶體電連接至該縮

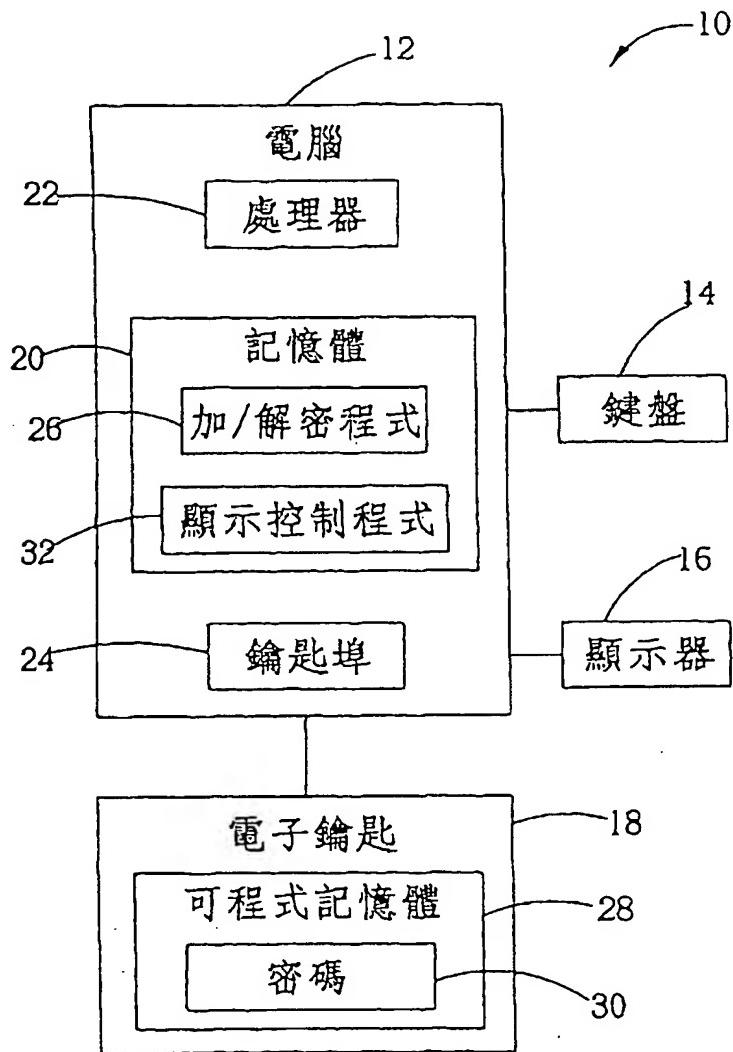
匙埠之上。

- 8.如申請專利範圍第1項之電腦系統，其中該記憶體另包含有一顯示控制程式用來將一程式或檔案以圖標(icon)形式顯示於該顯示器上，當該加／解密程式對一程式或檔案進行加密時，該顯示控制程式會將表示該程式或檔案之

圖標隱藏起來，而當該加／解密程式對該程式或檔案進行解密時，該顯示控制程式會將該程式或檔案以圖標形式顯示於該顯示器上。

5. 圖式簡單說明：

第一圖為本發明電腦系統之功能方塊圖。



第一圖

corresponding to

TW 420796



US006618807B1

(12) United States Patent
Wang et al.

(10) Patent No.: US 6,618,807 B1
(45) Date of Patent: Sep. 9, 2003

(54) COMPUTER SYSTEM WITH AN EXTERNAL AND PORTABLE ELECTRONIC KEY FOR ENCRYPTION AND DECRYPTION PROCESSES

5,432,851 A * 7/1995 Scheidt et al. 713/184
5,623,637 A * 4/1997 Jones et al. 710/13
5,937,063 A * 8/1999 Davis 713/187
6,038,320 A * 3/2000 Miller 380/44
6,094,486 A * 7/2000 Marchant 380/28
6,351,813 B1 * 2/2002 Mooney et al. 380/259

(75) Inventors: Han-Che Wang, Taipei (TW);
Ming-Chih Chang, Taipei (TW)

(73) Assignee: Primax Electronics Ltd., Taipei Hsien (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: 09/275,086

(22) Filed: Mar. 24, 1999

(30) Foreign Application Priority Data

Jan. 13, 1999 (TW) 88100448 A

(51) Int. Cl.⁷ G06F 11/30; G06F 12/14;
H04L 9/32

(52) U.S. Cl. 713/189; 713/185; 713/202;
380/259; 380/278; 380/283

(58) Field of Search 380/44, 259, 278,
380/283; 713/186, 185, 184, 189

(56) References Cited

U.S. PATENT DOCUMENTS

4,599,489 A * 7/1986 Cargile 705/52
5,323,465 A * 6/1994 Avarne 713/184

OTHER PUBLICATIONS

PR Newswire, "Tritheim Technologies Announces a Fully-Integrated Security Solution for PCs PC Defender Utilizes Smart Card Technology to Protect Computer Access and Data", Nov. 16, 1998.*

* cited by examiner

Primary Examiner—Gilberto Barron

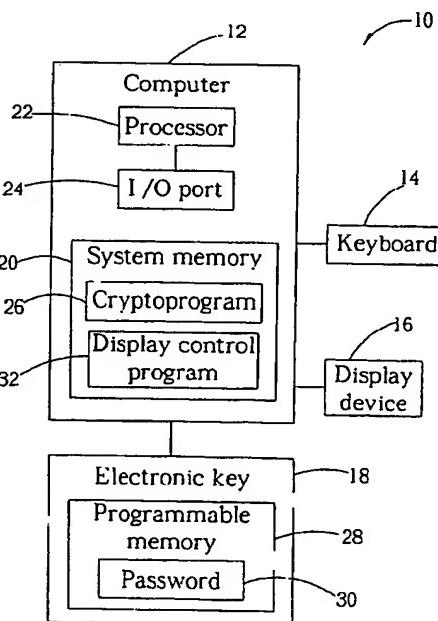
Assistant Examiner—Christopher J. Brown

(74) Attorney, Agent, or Firm—Winston Hsu

(57) ABSTRACT

The present invention provides a computer system comprising a system memory, a processor, a cryptoprocessor, an I/O port, and an electronic key. The electronic key can be inserted into and removed from the I/O port and contains a programmable memory that stores passwords. The cryptoprocessor is used to encrypt and decrypt programs or files stored in the system memory. Encryption of programs or files is accomplished according to a password that is stored in the programmable memory of the electronic key. During decryption, the cryptoprocessor searches for the corresponding password in the programmable memory of the key and decrypts the program or file if the password is found.

7 Claims, 1 Drawing Sheet



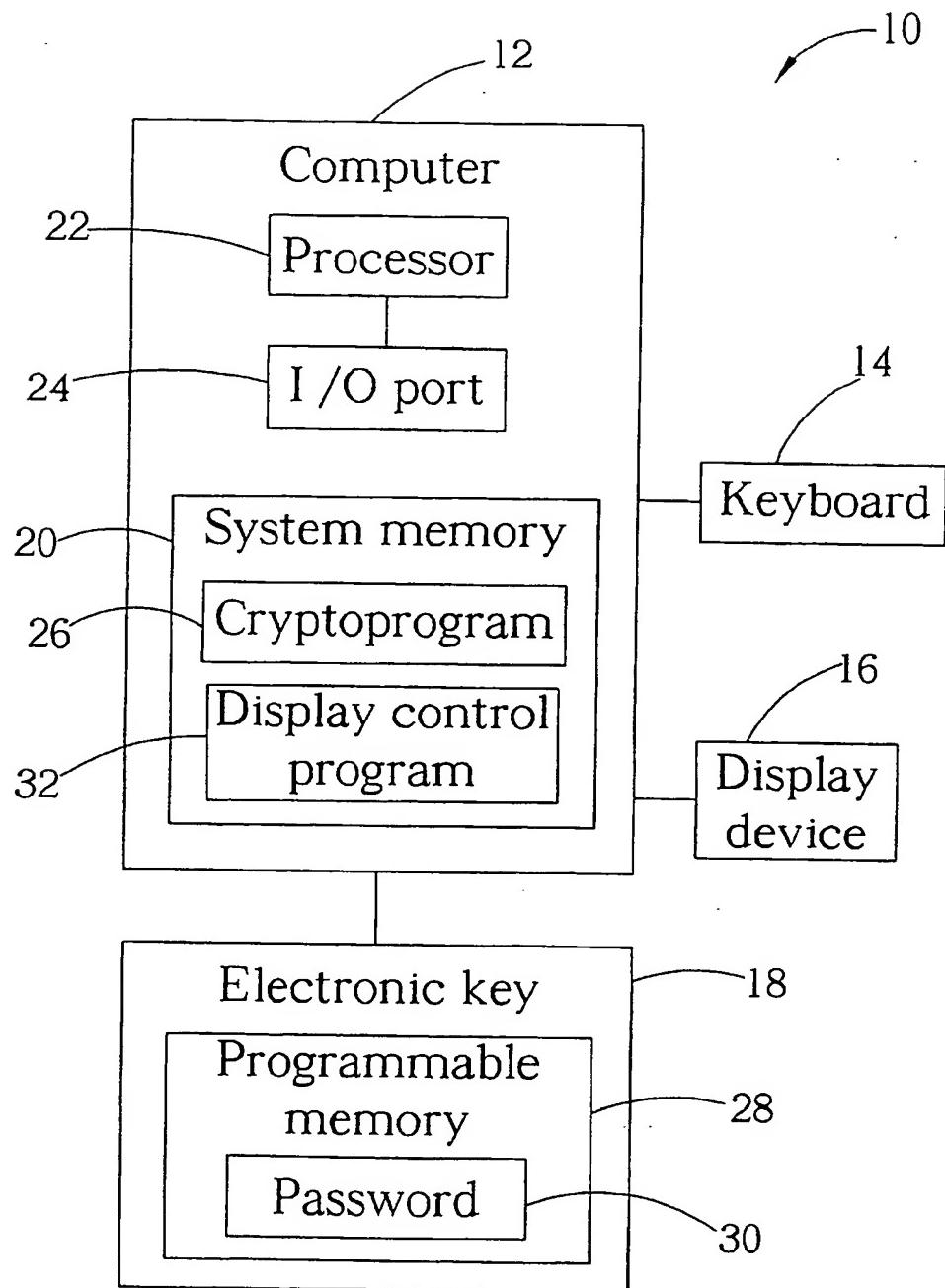


Fig. 1

**COMPUTER SYSTEM WITH AN EXTERNAL
AND PORTABLE ELECTRONIC KEY FOR
ENCRYPTION AND DECRYPTION
PROCESSES**

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to a computer system, and more particularly, to a computer system with a portable electronic key.

2. Description of the Prior Art

Data encryption of a computer system is commonly performed by using either software or hardware techniques. An example of a software technique is performed by using a cryptoprocessor. Unfortunately, cryptoprocessors can be easily broken through thus making all data insecure. In terms of techniques of maintaining data security by using hardware, a hardware key is popularly used. However, the hardware key is difficult to be disconnected from the computer system and is inconvenient to be carried around. Therefore, users often leave it on the computer system. This makes the hardware key easily accessible to others to steal or to reproduce thus compromising security.

SUMMARY OF THE INVENTION

It is therefore a primary objective of the present invention to provide a computer system with a portable electronic key to solve the above mentioned problems.

Briefly, in a preferred embodiment, the present invention provides a computer system comprising:

- a system memory for storing programs and files;
- a processor for executing the programs stored in the system memory;
- a cryptoprocessor for encrypting or decrypting a program or file stored in the system memory;
- an I/O (input/output) port connected to the processor; and
- an electronic key which can be inserted into and removed from the I/O port comprising a programmable memory for storing passwords;

wherein when encrypting a program or file stored in the system memory, the cryptoprocessor encrypts the program or file according to a password and stores the password in the programmable memory of the electronic key, and when decrypting a program or file stored in the system memory, the cryptoprocessor searches for a corresponding password in the programmable memory of the key and decrypts the program or file if the corresponding password is found.

It is an advantage of the present invention that the computer system according to the present invention uses an electronic key and a cryptoprocessor for enhancing data security. The password is stored in the electronic key which is separate from the computer thus securing the data.

These and other objects and the advantages of the present invention will no doubt become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiment that is illustrated in the various figures and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a functional block diagram of a computer system according to the present invention.

**DETAILED DESCRIPTION OF THE
PREFERRED EMBODIMENT**

Please refer to FIG. 1. FIG. 1 is a functional block diagram of a computer system 10 according to the present

invention. The computer system 10 comprises a computer 12, a display device 16, a keyboard 14, and a portable electronic key 18. The computer 12 comprises a system memory 20 for storing programs and files, a processor 22 for executing the programs stored in the system memory 20, an I/O (input/output) port 24 connected to the processor 22, a cryptoprocessor 26 stored in the system memory 20 for encrypting or decrypting a program or file, and a display control program 32 stored in the system memory 20 for displaying a program or file on the display device 16 in the form of an icon. The user can use the keyboard 14 for inputting a password to the cryptoprocessor 26 or changing a password used by the cryptoprocessor 26.

The electronic key 18 can be inserted into and removed from the I/O port 24, and it comprises a programmable memory 28 for storing passwords 30. The programmable memory 28 of the electronic key 18 is an EEPROM (electrically erasable programmable read only memory). The electronic key 18 can be any portable device or peripheral of a computer. For example, the electronic key 18 can be a mouse which can generate cursor control signals with the I/O port 24 being a serial port for connecting the mouse. The electronic key 18 can also be a memory card with a connector installed at its front end for connecting the programmable memory 28 to the I/O port 24 with the I/O port 24 being a USB (universal serial bus) port for plugging in the memory card. The electronic key 18 can also be a keypad, or any other I/O device.

When encrypting a program or file stored in the system memory 20, a user must connect the electronic key 18 to the I/O port 24 and input a password 30 by using the keyboard 14. The cryptoprocessor 26 will then encrypt the program or file according to the password 30 and store the password 30 in the programmable memory 28 of the electronic key 18. Under these circumstances, the display control program 32 will not display the icon representing the program or file. In this way, the file or program is effectively hidden.

When decrypting a program or file, the user must connect the electronic key 18 to the I/O port 24 and input a password 30 by using the keyboard 14. The cryptoprocessor 26 then searches for a corresponding password 30 in the programmable memory 28 of the key 18. If the inputted password is the same as the password 30 previously inputted when encrypting, the cryptoprocessor 26 will decrypt the program or file according to the password 30, and the display control program 32 will display the icon representing the program or file on the display device 16. If the inputted password is different from the password 30, the cryptoprocessor 26 will not find the corresponding password 30 in the programmable memory 28, and the display control program 32 will not display the icon representing the program or file on the display device 16.

The computer system 10 uses an electronic key 18 and a cryptoprocessor 26 for performing data encryption, thus both hardware and software techniques are employed to improve data security. Moreover, because the electronic key 18 such as a mouse or a memory card can be easily disconnected from the I/O port 24 and is portable, it can be removed from the I/O port 24 to prevent reproduction or stealing. Furthermore, the password 30 is stored in the programmable memory 28 of the electronic key 18, thus the password 30 cannot be searched unless the electronic key 18 is connected to the I/O port 24. Therefore data security is greatly enhanced.

In contrast to the prior art computer system, the computer system 10 according to the present invention uses an elec-

tronic key 18 that is removable from the computer and a cryptoprogram 26 for data security with the password being stored in the electronic key 18, not the computer 12. Therefore, data security is assured.

Those skilled in the art will readily observe that numerous modifications and alterations of the system may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.

Those skilled in the art will readily observe that numerous modifications and alterations of the system may be made while retaining the teachings of the invention. Accordingly, the above disclosure should be construed as limited only by the metes and bounds of the appended claims.

What is claimed is:

1. A computer system comprising:
a system memory for storing programs, files, and a display control program for displaying the programs or files stored in the system memory on a display device in the form of an icon;
a processor connected to the display device for executing the programs stored in the system memory;
a cryptoprogram for encrypting or decrypting a program or file stored in the system memory;
an I/O (input/output) port connected to the processor; and
an electronic key which can be inserted into and removed from the I/O port comprising a programmable memory for storing passwords;
wherein when encrypting a program or file stored in the system memory, the cryptoprogram encrypts the pro-

gram or file according to a password and stores the password in the programmable memory of the electronic key, and the display control program conceals the icon representing the program or file, and when decrypting a program or file stored in the system memory, the cryptoprogram searches for a password corresponding to the program or file in the programmable memory of the key and decrypts the program or file if the corresponding password is found, and the display control program displays the icon representing the program or file on the display device.

2. The computer system of claim 1 further comprising an input device connected to the processor for inputting a password to the cryptoprogram or changing a password used by the cryptoprogram.
3. The computer system of claim 2 wherein the input device is a keyboard.
4. The computer system of claim 1 wherein the programmable memory of the electronic key is an EEPROM.
5. The computer system of claim 1 wherein the I/O port is a serial port or a universal serial bus (USB) port.
6. The computer system of claim 1 wherein the key is built in a mouse which can be used for generating pointing signals.
7. The computer system of claim 1 wherein the key is a memory card with an electrical connector for electrically connecting the programmable memory in the key to the I/O port.

* * * * *